ConnectWise SOC Statement of Work

1. Overview

This Statement of Work (“SOW”) for the Global Security Operations Center (“SOC”) Service has been entered into pursuant to the Schedule of Software and Services ("Schedule") between your organization (“You,” “Your” “MSP” or “Client”) and the ConnectWise Affiliate identified on the Schedule and is subject to the terms of the then current Master Agreement and the applicable Addendum(s) located at www.connectwise.com/legal (collectively the "Agreement"). Such terms are incorporated by reference as if fully set forth herein.

This SOW is ConnectWise confidential and proprietary information. This SOW may change and ConnectWise may update this SOW from time to time. It is your responsibility to check this SOW periodically for changes.

2. Service Description

ConnectWise’s SOC Service provides monitoring, detection, investigation, escalation, and incident support for incidents within the current support toolset and visibility of the managed services. This SOW defines what is in scope, what is not in scope, and client responsibilities. The Client acknowledges and agrees that anything not specifically set forth herein as in scope is deemed out of scope. “End Client” or “End Client site” shall mean any entity for whom the MSP provides one or more elements of the SOC offering.

3. SOC Services

SOC Services vary based on the security products purchased. Product specific variations will be defined in the "In Scope Services" section of this SOW. The following service definitions are common to all services.

Coverage Hours

24x7: 24 hours a day, 7 days a week coverage

Location of Services

ConnectWise has multiple offices for SOC Service teams including Tampa, FL, USA, Pittsburgh, PA, USA, Pune, India and Mumbai, India. ConnectWise also hires technicians via a work from home policy.

4. In Scope Services

Incident Investigation and Response

The SOC will provide monitoring, detection, investigation, escalation, and incident support for all incidents within the current supported toolset and visibility of the services.

The SOC is responsible for remote incident analysis and investigation to determine if alerts or security events warrant incident classification. If an event is classified as an incident by the SOC,

the SOC will track the incident with You. The SOC will perform incident triage to include determining threat scope, urgency, and potential impact and make recommendations designed to allow for remediation.

The SOC will remotely investigate initial security events identified by the SOC and escalate as appropriate in all accordance with the established and agreed upon Service Level Objectives (SLOs) for the security products purchased. Events and incidents will be analyzed and investigated using the SOC's standard processes and procedures. Escalations will follow established escalation paths and utilize contact information collected during onboarding and documented by SOC.

For incidents that are assigned to the Client after analysis, the Client is responsible for escalating incidents back to the SOC that Client requires further action or analysis by the SOC.

The SOC will be the collection point for additional group inputs for the classification of security incidents. The potential exists for other entities (other ConnectWise services, external IR teams, etc.) to notify the SOC of possible events. In these relatively rare cases, the SOC will ensure outside sources of information are incorporated into established SOC workflow procedures. As events are pulled into the SOC Workflow, it is the SOC's responsibility to create and classify incidents. As the SOC is responsible for incident escalation and response, only the SOC has the authority to classify events or alerts as incidents to ensure due diligence of event investigation and accountability in reporting.

During incident investigation the SOC may perform the following activities:

- Perform analysis on client assets/traffic, document results noting attacker profiles.
- Assist in identifying potential impact of incidents on client systems and using available ConnectWise security tools to assist client in determining if data was exfiltrated.
- Document and track events (false positives and false negatives, blacklists, whitelists) within the ConnectWise security toolset.
- Escalate incidents to identified client contacts for further remediation.

Testing of Monitoring and Response Capabilities

The Client may test SOC monitoring and response capabilities by staging simulated or actual reconnaissance activity, system or network attacks, and/or system compromises. Such activities may be initiated directly by Client or by a contracted third party. Client shall notify the SOC testing email at least fourteen (14) days in advance of testing with the expectation that analyst activities will not be notified of testing. Testing performed on newly added (within 60 days) assets or data feeds should be communicated to the SOC via advance electronic or written notice to ensure SOC personnel have properly onboarded new information and that all monitoring and response capabilities are working properly. SLOs will not apply during the period of staged or testing activities.

Scheduled and Emergency Maintenance

Scheduled maintenance means any maintenance that is performed during a scheduled maintenance window or in which Client is notified at least one day in advance. Notice of scheduled maintenance will be provided to the Client's Authorized Point of Contact. Emergency maintenance means any non-scheduled, non-standard maintenance required by SOC. No statement in the section of any Services entitled "Service Level Objectives" shall prevent SOC from conducting emergency maintenance if it is critically necessary for the integrity and security of the Services. During such emergency maintenance, Client's Authorized Point of Contact will receive notification of initialization of the emergency maintenance, and of the completion of the emergency maintenance. The SOC will be relieved of its obligations under the applicable SLOs during scheduled and emergency maintenance.

File Sample Submissions

The SOC services may detect suspicious or malicious executable files on endpoints. Sometimes it is necessary to perform additional investigations to understand an attack. In these cases, ConnectWise may retrieve file samples of suspicious or malicious files from an endpoint to perform additional analysis.

By allowing sample submissions, our analysts are enabled to provide more in-depth analysis and context to their investigations of potential incidents, as well as enhancing the detection and prevention of future incidents that may involve the same file(s).

Part of this process may require our analysts to request samples of files, scripts, or other source detected in Client or End Client environments to perform further analysis. In addition to our in-house analysis, ConnectWise may use outside services.

Unless the Client opts out of File Analysis Submissions, the SOC will request samples from an endpoint and upload potentially malicious files for analysis as needed.

By allowing permission for the SOC to upload unknown binaries, SOC Analysts will either manually or automatically upload unknown binaries to outside analysis services:

- Sample binary or its hash representation will be submitted to the appropriate analysis service.
- Terms of Service and Privacy Policy for each service will apply.
- The SOC shall not be responsible for this submission or for any act or omission by any online service.

You are hereby advised some/most analysis services make the file metadata publicly available, along with scan results from numerous anti-virus products. Service providers may also make the file samples available for download to partners.

5. Service Specific In Scope Services

MDR Services

Host Isolation Terms

With our MDR offerings, ConnectWise SOC has the ability to isolate machines on a Client or End Client's network that have an agent installed (i.e., SentinelOne, Bitdefender, Microsoft®). The SOC uses host isolation to prevent the spread of malicious code by preventing a compromised machine from communicating to other network devices on the Internet or the Client or End Client's network. The isolated machine will maintain connectivity to SOC and allow our analysts to continue the investigation without risking other network devices to malicious code or active attacks.

The ConnectWise SOC also has the ability with some services to block connectivity from devices without an agent installed (Microsoft). The SOC uses containment to keep potentially compromised unmanaged machines from talking to managed machines. The contained machine will be unable to communicate with any device with an agent installed.

Unless the Client opts-out, ConnectWise will isolate and/or contain potentially compromised machines. ConnectWise will manually isolate/contain the machine using the installed Endpoint Agent and notify the client of the isolation via an incident for escalation. The machines will remain in isolation until the threat has been remediated or the client has specifically said they accept the risk and requests the SOC to remove the isolation.

- The client commits to identifying production impacting servers and assets that are NOT to be isolated unless the client has given written authorization. Client recognizes they assume all risk for non-isolated machines and the spread of any attack profile due to this.
- The SOC commits to isolating/containing machines that are NOT on the unauthorized list only to prevent the spread of malicious code and lateral movement by suspected attackers.
- The SOC will escalate all incidents that require isolation/containment to the client for their visibility and active feedback on the incident.

Clients are hereby advised that the SOC has the functionality to isolate/contain machines on your network or End Client's network with installed CW MDR offerings, that the SOC has the ability to use this function to protect the network, and that the isolated machines will lose all connectivity to all other devices on the network and the contained machines will lose all connectivity to all other SOC managed devices on the network.

Automated Remediation

Some incidents can be remediated by the ConnectWise MDR agents. These remediation actions are visible in the endpoint console.

Clients can opt out of allowing SOC Analysts to execute the automated remediation actions on affected endpoints. The current remediation actions that can be performed are, but are not limited to:

- SentinelOne
    - Run Scan

    - Kill Process
    - Quarantine Files
    - Remediate Threat
    - Rollback Threat
- Bitdefender
    - Stop Process
    - Quarantine Files
    - Isolate Device
- Microsoft
    - Run Scan
    - Collect Investigation Package
    - Stop Process
    - Quarantine Files
    - Restrict App Execution
    - Isolate Device
    - Contain Device

Clients are hereby advised that the SOC has the functionality to remediate machines on your or your End Client's network, that the SOC can use this function to protect the network, and that the SOC is not liable for downtime as the result of remediation actions that were taken.

6. Out of Scope Services

The following is out of scope:

1. The SOC Service does not modify network configurations, including firewalls, nor does it provide support for troubleshooting network performance or function.
2. Fix database corruption issues.
3. SOC Service will not perform any virtualizations on a backup solution.
4. End Client Training.
5. Contacting third party vendors for support or security involvement.
6. Under no circumstance will the SOC Service engage in financial transactions on Client's behalf.

7. Hardware-related issues (i.e., hard disk, memory, power supply). All hardware and/or equipment issues will be escalated to the Client for remediation.
8. Issues detected with ConnectWise's non-security platforms.
9. Internet service provider (ISP) outages.
10. Hardware, software, or ISP vendor ticketing and management.
11. On-site support at client and/or end client locations.
12. Anything not specifically identified as in scope.

7. Client Responsibilities

Client understands that SOC's performance of the services is dependent in part on the Client's compliance with the requirements of this SOW. The Client understands that it is responsible for timely delivery of the items and information listed in the following sections of this SOW. Additionally, the Client understands that it must perform the tasks, and provide access to Client or End Client's employees, consultants, business processes, and/or systems as contemplated herein for SOC to be able to perform such services efficiently. The following list is required for the SOC's ability to perform the Services.

The Client shall provide reasonable assistance to the SOC for performance under this SOW, including helping troubleshoot technical issues within the Client or End Client's environments as well as any services provided by third parties to the Client that may affect the delivery of the Services.

SOC services are dependent on the connectivity of the tools utilized. Client is responsible for maintaining a proper Internet connection sized appropriately to handle the load of ConnectWise tools and monitoring activities on their network and any End Client network supported by the SOC services.

Provide SOC with accurate and up-to-date information including, the name, email, landline, and mobile numbers for all designated authorized Client Points(s) of Contact ("POC(s)"). SOC will also supply an accurate and up-to-date list of its POCs for Client. Notify ConnectWise at least twenty-four (24) hours in advance of any scheduled maintenance, network or system administration activity that would affect SOC's ability to perform under this SOW.

Maintaining current maintenance, supported versions and technical support contracts with Client's software and hardware vendors for any device affected by this SOW.

Client is responsible for maintaining ConnectWise products installed on Client or End Client's networks on currently supported versions and monitoring that any EDR endpoint agent stays in an online state

Client Environment Failures

The Client agrees that ConnectWise will not be liable for any failure to provide the SOC Services if such failure is caused by Client's failure to meet the applicable requirements for each Service.

At a minimum, Client is responsible for ensuring the following environmental failures do not negatively impact the Services:

- Service interruptions, deficiencies, degradations or delays due to any Client or End Client supplied internet or private access whether provided by Client, End Client or third parties engaged by Client or End Client, or equipment when provided by Client, End Client or third parties engaged by Client or End Client.
- Failure or deficient performance of Client-supplied or End Client-supplied power, equipment, services, or systems not provided by ConnectWise.
- Client or End Client's election to not release a service component for testing and/or repair and to continue using the service component.
- Client or End Client's failure to adhere to SOC recommended configurations on managed or unmanaged equipment that affects the Service.
- Client's failure to deploy SOC Agents within monitored networks.
- Service interruptions, deficiencies, degradations, or delays during any period when a service component is removed from Service for maintenance, replacement, or rearrangement purposes by Client's submission without a mutually agreed upon change order form.
- Failure to provide a suitable secure environment for on-premise devices, including, but not limited to secure mounting/racking, appropriate cooling and air handling, secure from theft, loose wires bundled neatly, etc.
- Service interruptions, deficiencies, degradations, or delays in Service caused by a piece of equipment, configuration, routing event or technology required to be operative in order to perform under this SOW that is under the management and control of Client or End Client.

8. Service Level Objectives:

ConnectWise endeavors to provide the following service levels:

- MDR Initial Threat Analysis SLO: Completed within 1 hour of alert, includes initial investigation, containment (if necessary) and escalation (if necessary).
- ConnectWise SIEM™ Initial Threat Analysis SLO: Completed pursuant to product SKU SLO applied to supported site. Includes initial investigation and escalation (if necessary).
- Client Created Ticket Initial Response SLO: Varies by priority (Low – 4 hour, Medium – 4 hour, High – 2 hour, Urgent – 1 hour). All email initiated tickets originate as low priority.
- Voicemail Response: All voicemails to the SOC are classified as Urgent tickets with a 1 hour initial response goal.

9. How to contact the SOC Service

Client can contact the SOC via Phone, Email, or Chat using the methods listed below. ConnectWise prioritizes incoming real-time alerts, phone calls, and chats utilizing the SLOs listed above:

- For Critical Incident Support utilize our chat service on our support portal at https://support.carvir.net or call our SOC Client Support telephone numbers at:
    - US and Canada: 770-742-7700
    - UK and EMEA: +44 (0)203-817-6911
    - Australia and New Zealand: +61 283-304-888
- For non-urgent requests open tickets by emailing our dedicated SOC Client support address at securitypartnersupport@connectwise.com

Client shall not initiate calls or chats directly with individual ConnectWise SOC Service technicians on their private lines.

SOC interaction is limited to Client engagement and is not for the purpose of End Client engagement. At times the SOC will work with the Client to communicate with End Clients on specific issues, but this is always in conjunction with the Client. The support methods listed in this section are not to be shared with the End Client for direct engagement with the SOC.

The following are the options available to the Client for changing the prioritization or checking the status of a ticket:

- Change the priority via the Freshdesk ticket portal (Preferred Method)
- Call our SOC Client Support telephone number
- Email our dedicated SOC Client support address at securitypartnersupport@connectwise.com

10. Revision History

Document Version	Date Published	Revision Description	Notes
2.02	10/19/2021	Reformatted and Simplified Structure of the document.	
3	9/8/2023	Added Service Specific In Scope Services section.	
2.04	1/31/2025	Updated for new service offerings.	